

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSA) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat adobe -- reader	Unspecified vulnerability in Adobe Reader and Adobe Acrobat 9.1 and 7.1.1 allows remote attackers to execute arbitrary code via unknown vectors related to a JavaScript method and input validation, a different vulnerability than CVE-2009-0658.	2009-03-19	10.0	CVE-2009-0927 CONFIRM
autonomy -- keyview_export_sdk autonomy -- keyview_filter_sdk autonomy -- keyview_viewer_sdk ibm -- lotus_notes symantec -- altiris_deployment_solution symantec -- brightmail symantec -- data_loss_prevention_detection_servers symantec -- data_loss_prevention_endpoint_agents symantec -- enforce symantec -- mail_security	Stack-based buffer overflow in wp6sr.dll in the Autonomy KeyView SDK 10.4 and earlier, as used in IBM Lotus Notes, Symantec Mail Security (SMS) products, Symantec BrightMail Appliance products, and Symantec Data Loss Prevention (DLP) products, allows remote attackers to execute arbitrary code via a crafted Word Perfect Document (WPD) file.	2009-03-18	9.3	CVE-2008-4564 CONFIRM XF VUPEN VUPEN VUPEN CONFIRM BID CONFIRM SECTRACK SECTRACK SECUNIA SECUNIA SECUNIA SECUNIA OSVDB IDEFENSE
	Multiple SQL injection vulnerabilities in Beerwin			CVE-2009-1024

beerwin -- phplinkadmin	PHPLinkAdmin 1.0 allow remote attackers to execute arbitrary SQL commands via the linkid parameter to edlink.php, and unspecified other vectors.	2009-03-19	7.5	XF VUPEN BID MILWORM SECUNIA
beerwin -- phplinkadmin	PHP remote file inclusion vulnerability in linkadmin.php in Beerwin PHPLinkAdmin 1.0 allows remote attackers to execute arbitrary PHP code via a URL in the page parameter.	2009-03-19	7.5	CVE-2009-1025 XF VUPEN BID MILWORM SECUNIA
deluxeBB -- deluxeBB	SQL injection vulnerability in misc.php in DeluxeBB 1.3 and earlier allows remote attackers to execute arbitrary SQL commands via the qorder parameter, a different vector than CVE-2005-2989 and CVE-2006-2503.	2009-03-20	7.5	CVE-2009-1033 BID MILWORM
denis_moinel -- phpgkit	PHP remote file inclusion vulnerability in connexion.php in PHPGKit 0.9 allows remote attackers to execute arbitrary PHP code via a URL in the DOCUMENT_ROOT parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-19	7.5	CVE-2008-6491 XF MISC BID
dflabs -- ptk	Multiple unspecified vulnerabilities in DFLabs PTK 1.0.0 through 1.0.4 allow remote attackers to execute arbitrary commands in processes launched by PTK's Apache HTTP Server via (1) "external tools" or (2) a crafted forensic image.	2009-03-16	7.5	CVE-2009-0918 CONFIRM CERT-VN
dflabs -- ptk	DFLabs PTK 1.0.0 through 1.0.4 has (1) "lamp" as its default password for the "nobody" account within the included ProFTPD installation, and possibly has (2) a blank default password for the "root" account within the included MySQL installation, which makes it easier for remote attackers to obtain access. NOTE: the vendor states that the product is intended for use in a laboratory with "no contact from / to internet."	2009-03-16	7.5	CVE-2009-0919 CONFIRM
digiappz -- digiaffiliate	Multiple SQL injection vulnerabilities in login.asp in Digiappz DigiAffiliate 1.4 and earlier allow remote attackers to execute arbitrary SQL commands	2009-03-18	7.5	CVE-2008-6487 XF BID

	via the (1) admin and (2) password fields.			MILWORM
drupal -- tasklist	SQL injection vulnerability in the Tasklist module 5.x-1.x before 5.x-1.3 and 5.x-2.x before 5.x-2.0-alpha1, a module for Drupal, allows remote attackers to execute arbitrary SQL commands via values in the URI.	2009-03-20	10.0	CVE-2009-1034 CONFIRM
edisy -- ezip_wizard	Stack-based buffer overflow in ediSys eZip Wizard 3.0 allows remote attackers to execute arbitrary code via a crafted .zip file.	2009-03-19	9.3	CVE-2009-1028 XF MILWORM
fahlstad -- fmblog_plugin	SQL injection vulnerability in fmblog.php in the fMoblog plugin 2.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php. NOTE: some of these details are obtained from third party information.	2009-03-19	7.5	CVE-2009-0968 VUPEN BID MILWORM SECUNIA
flysforum -- flaber	function/update_xml.php in FLABER 1.1 and earlier allows remote attackers to overwrite arbitrary files by specifying the target filename in the target_file parameter. NOTE: this can be leveraged for code execution by overwriting a PHP file, as demonstrated using function/upload_file.php.	2009-03-19	7.5	CVE-2008-6490 XF VUPEN MILWORM
futomi -- mp_form_mail_cgi	Unspecified vulnerability in Futomi's CGI Cafe MP Form Mail CGI eCommerce 1.3.0 and earlier, and CGI Professional 3.2.2 and earlier, allows remote attackers to gain administrative privileges via unknown attack vectors.	2009-03-18	7.5	CVE-2009-0962 XF XF BID CONFIRM SECUNIA OSVDB JVNDB JVN
go-evolution -- evolution-data-server	Multiple integer overflows in Evolution Data Server (aka evolution-data-server) before 2.24.5 allow context-dependent attackers to execute arbitrary code via a long string that is converted to a base64 representation in (1) addressbook/libebook/e-vcard.c in evc or (2) camel/camel-mime-utils.c in libcamel.	2009-03-14	7.5	CVE-2009-0587 BID MLIST MISC MISC
	Heap-based buffer overflow in the			CVE-2009-

<p>gomlab -- gom_encoder</p>	<p>Preview/ Set Segment function in Gretech GOMlab GOM Encoder 1.0.0.11 and earlier allows user-assisted remote attackers to cause a denial of service (memory corruption and application crash) or execute arbitrary code via a long text field in a subtitle (.srt) file.</p>	<p>2009-03-19</p>	<p>9.3</p>	<p>1022 XF BID BUGTRAQ MILWORM MISC SECUNIA OSVDB</p>
<p>gststreamer -- gst-plugins-base</p>	<p>Integer overflow in the gst_vorbis_tag_add_coverart function (gst-libs/gst/tag/gstvorbistag.c) in vorbistag in gst-plugins-base (aka gststreamer-plugins-base) before 0.10.23 in GStreamer allows context-dependent attackers to execute arbitrary code via a crafted COVERART tag that is converted from a base64 representation, which triggers a heap-based buffer overflow.</p>	<p>2009-03-14</p>	<p>7.5</p>	<p>CVE-2009-0586 BID MLIST MISC</p>
<p>hp -- 8100c_digital_sender hp -- 9100c_digital_sender hp -- 9200c_digital_sender hp -- 9250c_digital_sender hp -- color_laserjet hp -- color_laserjet_1500 hp -- color_laserjet_2500 hp -- color_laserjet_2500l hp -- color_laserjet_2500lse hp -- color_laserjet_2500n hp -- color_laserjet_2500tn hp -- color_laserjet_2605dtn hp -- color_laserjet_4370mfp hp -- color_laserjet_4600 hp -- color_laserjet_4650 hp -- color_laserjet_4700 hp -- color_laserjet_4730_mfp hp -- color_laserjet_5550 hp -- color_laserjet_8500 hp -- color_laserjet_8550 hp -- color_laserjet_9500 hp -- color_laserjet_9500_mfp hp -- color_laserjet_9500mfp hp -- color_mfp_cm8050 hp -- color_mfp_cm8060 hp -- digital_senders hp -- edgeline_printers hp -- laserjet hp -- laserjet_2200 hp -- laserjet_2200dtn hp -- laserjet_2300dn hp -- laserjet_2410 hp -- laserjet_2420 hp -- laserjet_2430</p>				

<p>hp -- laserjet_2500 hp -- laserjet_2500c hp -- laserjet_2600c hp -- laserjet_2600n hp -- laserjet_3000 hp -- laserjet_3700 hp -- laserjet_4 hp -- laserjet_4000 hp -- laserjet_4000n hp -- laserjet_4050 hp -- laserjet_4100_mfp hp -- laserjet_4100mfp hp -- laserjet_4200 hp -- laserjet_4200dnt_network_printer hp -- laserjet_4200ln hp -- laserjet_4250 hp -- laserjet_4300 hp -- laserjet_4345_mfp hp -- laserjet_4345mfp hp -- laserjet_4350 hp -- laserjet_4350dtn hp -- laserjet_4650dn hp -- laserjet_4m_plus hp -- laserjet_5 hp -- laserjet_5000 hp -- laserjet_5000_printer hp -- laserjet_5100 hp -- laserjet_5100dtn hp -- laserjet_5m hp -- laserjet_8150dn hp -- laserjet_9000 hp -- laserjet_9000_mfp hp -- laserjet_9000mfp hp -- laserjet_9040 hp -- laserjet_9040_mfp hp -- laserjet_9040_mpf hp -- laserjet_9040mfp hp -- laserjet_9050 hp -- laserjet_9050_mfp hp -- laserjet_9050_mpf hp -- laserjet_9050mfp hp -- laserjet_9055 hp -- laserjet_9065 hp -- laserjet_9500 hp -- laserjet_9500_mpf hp -- laserjet_9500mfp hp -- laserjet_m1522n_mfp hp -- laserjet_m3027_mfp hp -- laserjet_m3035_mfp hp -- laserjet_m4345_mfp hp -- laserjet_m5025_mfp hp -- laserjet_m5035_mfp</p>	<p>The HP Embedded Web Server (EWS) on HP LaserJet Printers, Edgeline Printers, and Digital Senders has no management password by default, which makes it easier for remote attackers to obtain access.</p>	<p>2009-03-18</p>	<p>7.6</p>	<p>CVE-2009-0941 BUGTRAQ MISC HP</p>
<p>hucovin_hera_ahaci_com_myalbum</p>	<p>SQL injection vulnerability in MyAlbum component (com_myalbum) 1.0 for Joomla!</p>	<p>2009-03-</p>	<p>7.5</p>	<p>CVE-2008-6489 VE</p>

muscyim_dora_abacl -- com_myalbum	allows remote attackers to execute arbitrary SQL commands via the album parameter to index.php.	19	7.5	CVE-2009-0965 XF MILWORM
ismail_fahmi -- ganesha_digital_library	SQL injection vulnerability in functions/browse.php in Ganesha Digital Library (GDL) 4.0 and 4.2 allows remote attackers to execute arbitrary SQL commands via the node parameter in a browse action to gdl.php.	2009-03-19	7.5	CVE-2009-0965 XF MILWORM
joe_shaw -- libsoup	Integer overflow in the soup_base64_encode function in soup-misc.c in libsoup 2.x.x before 2.2.x, and 2.x before 2.24, allows context-dependent attackers to execute arbitrary code via a long string that is converted to a base64 representation.	2009-03-14	7.5	CVE-2009-0585 MISC
joomprod -- com_versioning	SQL injection vulnerability in the Versioning component (com_versioning) 1.0.2 in Joomla! and Mambo allows remote attackers to execute arbitrary SQL commands via the id parameter in an edit task to index.php.	2009-03-17	7.5	CVE-2008-6481 MISC
kim -- websites	Multiple SQL injection vulnerabilities in login.php in Kim Websites 1.0 allow remote attackers to execute arbitrary SQL commands via the (1) username and (2) password parameters.	2009-03-19	7.5	CVE-2009-1026 MISC
mandriva -- multi_network_firewall mandriva -- linux mandriva -- linux_corporate_server	perl-MDK-Common 1.1.11 and 1.1.24, 1.2.9 through 1.2.14, and possibly other versions, in Mandriva Linux does not properly handle strings when writing them to configuration files, which allows attackers to gain privileges via "special characters" in unspecified vectors.	2009-03-16	7.2	CVE-2009-0912 MISC
miranda-im -- miranda_im	Stack-based buffer overflow in Miranda IM 0.6.8 allows remote attackers to execute arbitrary code via a crafted Yahoo! Messenger packet. NOTE: this might overlap CVE-2007-5590.	2009-03-18	9.3	CVE-2007-5542 MISC
miranda-im -- miranda_im	Stack-based buffer overflow in Miranda IM 0.6.8 and 0.7.0 allows remote attackers to execute arbitrary code via a crafted Yahoo! Messenger packet. NOTE: this might overlap CVE-2007-5590.	2009-03-18	9.3	CVE-2007-5543 MISC
	SQL injection vulnerability in			CVE-2008-

mole-group -- taxi_calc_dist_script	login.php in Mole Group Taxi Map Script (aka Taxi Calc Dist Script) allows remote attackers to execute arbitrary SQL commands via the user field.	2009-03-18	7.5	6484 XF BID MILWORM OSVDB
mumbojumbo -- op4	SQL injection vulnerability in Mumbo Jumbo Media OP4 allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php.	2009-03-16	7.5	CVE-2008-6477 XF VUPEN BID MILWORM
opencart -- opencart	SQL injection vulnerability in OpenCart 1.1.8 allows remote attackers to execute arbitrary SQL commands via the order parameter.	2009-03-19	7.5	CVE-2009-1027 XF BID BUGTRAQ MISC
opera -- opera opera_software -- opera_web_browser	Opera before 9.64 allows remote attackers to execute arbitrary code via a crafted JPEG image that triggers memory corruption.	2009-03-16	9.3	CVE-2009-0914 CONFIRM VUPEN CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM MLIST SECTrack GENTOO SECUNIA SECUNIA
opera -- opera opera_software -- opera_web_browser	Unspecified vulnerability in Opera before 9.64 has unknown impact and attack vectors, related to a "moderately severe issue."	2009-03-16	10.0	CVE-2009-0916 VUPEN CONFIRM CONFIRM CONFIRM CONFIRM SECUNIA
phpcomasy -- phpcomasy	SQL injection vulnerability in index.php in phpComasy 0.9.1 allows remote attackers to execute arbitrary SQL commands via the entry_id parameter.	2009-03-19	7.5	CVE-2009-1023 XF BID MILWORM
poppeeper -- pop_peeper	Stack-based buffer overflow in POP Peeper 3.4.0.0 and earlier allows remote POP3 servers to execute arbitrary code via a long Date header, related to Imap.dll.	2009-03-19	9.3	CVE-2009-1029 XF BID BUGTRAQ MILWORM MISC SECUNIA

rhinosoft -- serv-u	Directory traversal vulnerability in the FTP server in Rhino Software Serv-U File Server 7.4.0.1 allows remote attackers to create arbitrary directories via a \.. (backslash dot dot) in an MKD request.	2009-03-19	7.8	CVE-2009-1031 XF VUPEN MILWORM SECUNIA
softcomplex -- php_image_gallery	SQL injection vulnerability in index.php in SoftComplex PHP Image Gallery allows remote attackers to execute arbitrary SQL commands via the ctg parameter.	2009-03-18	7.5	CVE-2008-6485 XF BID MILWORM
softcomplex -- sharedlog	PHP remote file inclusion vulnerability in slideshow_uploadvideo.content.php in SharedLog, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the GLOBALS[root_dir] parameter.	2009-03-18	7.5	CVE-2008-6486 XF BID BUGTRAQ OSVDB
softcomplex -- php_image_gallery	SQL injection vulnerability in index.php in SoftComplex PHP Image Gallery 1.0 allows remote attackers to execute arbitrary SQL commands via the Admin field in a login action.	2009-03-18	7.5	CVE-2008-6488 BID MILWORM
sun -- opensolaris sun -- solaris	Unspecified vulnerability in Kerberos Incremental Propagation in Solaris 10 and OpenSolaris snv_01 through snv_110 allows remote attackers to cause a denial of service (loss of incremental propagation requests to slave KDC servers) via unknown vectors related to the master Key Distribution Center (KDC) server.	2009-03-17	7.8	CVE-2009-0923 VUPEN BID SUNALERT SECUNIA
tor -- tor	Tor before 0.2.0.34 treats incomplete IPv4 addresses as valid, which has unknown impact and attack vectors related to "Spec conformance," as demonstrated using 192.168.0.	2009-03-17	10.0	CVE-2009-0939 SECUNIA MLIST
tp -- neostrada_livebox_adsl_router	The Neostrada Livebox ADSL Router allows remote attackers to cause a denial of service (network outage) via multiple HTTP requests for the /- URI.	2009-03-19	7.8	CVE-2008-6497 XF BID BUGTRAQ MILWORM SECUNIA OSVDB
	PHP remote file inclusion vulnerability in admin.googlebase.php in the Ecom			CVE-2008-

virtuemart-solutions -- com_googlebase	Solutions VirtueMart Google Base (aka com_googlebase or Froogle) component 1.1 for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter.	2009-03-18	7.5	6483 BID MILWORM SECUNIA OSVDB
visagesoft -- expert_pdf_editorx	Insecure method vulnerability in the VSPDFEditorX.VSPDFEdit ActiveX control in VSPDFEditorX.ocx 1.0.200.0 in VISAGESOFT eXPert PDF EditorX allows remote attackers to create or overwrite arbitrary files via the first argument to the extractPagesToFile method.	2009-03-19	8.8	CVE-2008-6496 XF BID MILWORM SECUNIA
xlinesoft -- phprunner	Multiple SQL injection vulnerabilities in PHPRunner 4.2, and possibly earlier, allow remote attackers to execute arbitrary SQL commands via the SearchField parameter to (1) UserView_list.php, (2) orders_list.php, (3) users_list.php, and (4) Administrator_list.php.	2009-03-19	7.5	CVE-2009-0963 XF BID BUGTRAQ MILWORM MISC SECUNIA
yabsoft -- mega_file_hosting_script	PHP remote file inclusion vulnerability in cross.php in YABSoft Mega File Hosting 1.2 allows remote attackers to execute arbitrary PHP code via a URL in the url parameter. NOTE: this can also be leveraged to include and execute arbitrary local files via .. (dot dot) sequences.	2009-03-19	7.5	CVE-2009-0966 XF BID MILWORM SECUNIA
yabsoft -- advanced_image_hosting_script	SQL injection vulnerability in gallery_list.php in YABSoft Advanced Image Hosting (AIH) Script 2.3 allows remote attackers to execute arbitrary SQL commands via the gal parameter.	2009-03-20	7.5	CVE-2009-1032 BID MILWORM

[Back to top](#)

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Unspecified vulnerability in Sun Solaris 10 on SPARC sun4v systems, and OpenSolaris snv_47 through snv_85, allows local users to cause a denial of service (hang of UFS filesystem write) via unknown vectors related to the (1) ufs_getpage and (2) ufs_putapage routines, aka CR 6425723.	2009-03-17	4.7	CVE-2009-0925 VUPEN BID SUNALERT
	Cross-site request forgery (CSRF)			CVE-2008-

apachefriends -- xampp	vulnerability in security/xamppsecurity.php in XAMPP 1.6.8 allows remote attackers to change a certain .htaccess password via the xampppasswd parameter.	2009-03-19	6.8	6498 XF MILWORM SECUNIA
apachefriends -- xampp	security/xamppsecurity.php in XAMPP 1.6.8 performs an extract operation on the SERVER superglobal array, which allows remote attackers to spoof critical variables, as demonstrated by setting the REMOTE_ADDR variable to 127.0.0.1.	2009-03-19	5.5	CVE-2008-6499 XF MILWORM
apple -- itunes	Apple iTunes before 8.1 on Windows allows remote attackers to cause a denial of service (infinite loop) via a Digital Audio Access Protocol (DAAP) message with a crafted Content-Length header.	2009-03-14	5.0	CVE-2009-0016 CONFIRM APPLE
apple -- itunes	Apple iTunes before 8.1 does not properly inform the user about the origin of an authentication request, which makes it easier for remote podcast servers to trick a user into providing a username and password when subscribing to a crafted podcast.	2009-03-14	4.3	CVE-2009-0143 CONFIRM APPLE
codetoad -- asp_shopping_cart	Cross-site scripting (XSS) vulnerability in CodeToad ASP Shopping Cart Script allows remote attackers to inject arbitrary web script or HTML via the query string to the default URI.	2009-03-20	5.0	CVE-2008-6500 XF BID MISC
debian -- horde_imp	Multiple cross-site scripting (XSS) vulnerabilities in Horde IMP before 4.2.2 and 4.3.3 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors to (1) smime.php, (2) pgp.php, and (3) message.php.	2009-03-17	4.3	CVE-2009-0930 BID SECUNIA MLIST MLIST CONFIRM CONFIRM
debian -- horde debian -- horde_groupware	Cross-site scripting (XSS) vulnerability in the tag cloud search script (horde/services/portal/cloud_search.php) in Horde before 3.2.4 and 3.3.3, and Horde Groupware before 1.1.5, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-03-17	4.3	CVE-2009-0931 BID
debian -- horde debian -- horde_groupware	Directory traversal vulnerability in framework/Image/Image.php in Horde before 3.2.4 and 3.3.3 and Horde Groupware before 1.1.5 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the Horde_Image driver name.	2009-03-17	6.4	CVE-2009-0932 BID SECUNIA MLIST MLIST MLIST CONFIRM CONFIRM CONFIRM
	Cross-site scripting (XSS) vulnerability in			

dflabs -- ptk	DFLabs PTK 1.0.0 through 1.0.4 allows remote attackers to inject arbitrary web script or HTML by providing a forensic image containing HTML documents, which are rendered in web browsers during inspection by PTK. NOTE: the vendor states that the product is intended for use in a laboratory with "no contact from / to internet."	2009-03-16	4.3	CVE-2009-0917 MISC CERT-VN
dotclear -- dotclear	Cross-site scripting (XSS) vulnerability in the administrative interface in Dotclear before 2.1.5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-03-17	4.3	CVE-2009-0933 VUPEN CONFIRM
dotnetblogengine -- blogengine.net	Cross-site scripting (XSS) vulnerability in blog/search.aspx in BlogEngine.NET allows remote attackers to inject arbitrary web script or HTML via the q parameter.	2009-03-16	4.3	CVE-2008-6476 MISC OSVDB
drupal -- tasklist	Cross-site scripting (XSS) vulnerability in Tasklist module 5.x-1.x before 5.x-1.3 and 5.x-2.x before 5.x-2.0-alpha1, a module for Drupal, allows remote authenticated users to inject arbitrary web script or HTML via Cascading Style Sheets (CSS).	2009-03-20	5.0	CVE-2009-1035 BID CONFIRM
drupal -- plus1	Cross-site request forgery (CSRF) vulnerability in the Plus 1 module before 6.x-2.6, a module for Drupal, allows remote attackers to cast votes for content via unspecified aspects of the URI.	2009-03-20	5.8	CVE-2009-1036 BID CONFIRM
easy-news -- easy_content_management_publishing	Easy Content Management Publishing stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database via a direct request for Database/News.mdb.	2009-03-19	5.0	CVE-2008-6493 MILWORM
flashtux -- weechat	Wee Enhanced Environment for Chat (WeeChat) 0.2.6 allows remote attackers to cause a denial of service (crash) via an IRC PRIVMSG command containing crafted color codes that trigger an out-of-bounds read.	2009-03-19	5.0	CVE-2009-0661 BID
futomi -- access_analyzer_cgi	Cross-site scripting (XSS) vulnerability in futomi's CGI Cafe Access Analyzer CGI Standard Version 3.8.1 and earlier allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	2009-03-19	4.3	CVE-2009-0971 CONFIRM
gnome -- glib	Multiple integer overflows in glib/gbase64.c in GLib before 2.20 allow context-dependent attackers to execute arbitrary code via a long string that is converted either (1) from or (2) to a base64 representation.	2009-03-14	4.6	CVE-2008-4316 BID CONFIRM MLIST MISC
				CVE-2009-

<p>gnome -- evolution-data-server</p>	<p>The ntlm_challenge function in the NTLM SASL authentication mechanism in camel/camel-sasl-ntlm.c in Camel in Evolution Data Server (aka evolution-data-server) 2.24.5 and earlier, and 2.25.92 and earlier 2.25.x versions, does not validate whether a certain length value is consistent with the amount of data in a challenge packet, which allows remote mail servers to read information from the process memory of a client, or cause a denial of service (client crash), via an NTLM authentication type 2 packet with a length value that exceeds the amount of packet data.</p>	<p>2009-03-14</p>	<p>5.8</p>	<p>0582 CONFIRM XF VUPEN BID REDHAT REDHAT REDHAT SECTRACK SECUNIA SECUNIA SECUNIA SECUNIA OSVDB MLIST</p>
<p>hp -- digital_senders hp -- edgeline_printers hp -- laserjet</p>	<p>Multiple cross-site request forgery (CSRF) vulnerabilities in the HP Embedded Web Server (EWS) on HP LaserJet Printers, Edgeline Printers, and Digital Senders allow remote attackers to (1) print documents via unknown vectors, (2) modify the network configuration via a NetIPChange request to hp/device/config_result_YesNo.html/config, or (3) change the password via the Password and ConfirmPassword parameters to hp/device/set_config_password.html/config.</p>	<p>2009-03-18</p>	<p>5.1</p>	<p>CVE-2009-0940 BID BUGTRAQ MISC HP</p>
<p>ibm -- websphere_application_server</p>	<p>The Servlet Engine/Web Container component in IBM WebSphere Application Server (WAS) 5.1.0, 5.1.1.19, 6.0.2 before 6.0.2.35, 6.1 before 6.1.0.23, and 7.0 before 7.0.0.3 allows remote attackers to read arbitrary files contained in war files in (1) web-inf, (2) meta-inf, and unspecified other directories via unknown vectors, related to (a) web-based applications and (b) the administrative console.</p>	<p>2009-03-16</p>	<p>5.0</p>	<p>CVE-2009-0508 CONFIRM</p>
<p>justjoomla -- com_treeg</p>	<p>PHP remote file inclusion vulnerability in admin.treeg.php in the Flash Tree Gallery (com_treeg) component 1.0 for Joomla!, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via the mosConfig_live_site parameter.</p>	<p>2009-03-18</p>	<p>6.8</p>	<p>CVE-2008-6482 XF BID MILWORM SECUNIA OSVDB</p>
<p>linux -- kernel</p>	<p>The inotify_read function in the Linux kernel 2.6.27 to 2.6.27.13, 2.6.28 to 2.6.28.2, and 2.6.29-rc3 allows local users to cause a denial of service (OOPS) via a read with an invalid address to an inotify instance, which causes the device's event list mutex to be unlocked twice and prevents proper synchronization of a data structure for the inotify instance.</p>	<p>2009-03-17</p>	<p>4.7</p>	<p>CVE-2009-0935 MLIST</p>
				<p>CVE-2009-</p>

nucleus_group -- nucleus_cms	Directory traversal vulnerability in the media manager in Nucleus CMS before 3.40 allows remote attackers to read arbitrary files via unknown vectors.	2009-03-17	5.0	0929 XF VUPEN CONFIRM SECUNIA
opera -- opera opera_software -- opera_web_browser	Opera before 9.64 allows remote attackers to conduct cross-domain scripting attacks via unspecified vectors related to plug-ins.	2009-03-16	4.3	CVE-2009-0915 VUPEN CONFIRM CONFIRM CONFIRM CONFIRM SECUNIA
parallels -- virtuozzo_containers	Cross-site request forgery (CSRF) vulnerability in the file manager in the VZPP web interface for Parallels Virtuozzo 365.6.swsoft (build 4.0.0-365.6.swsoft) and 25.4.swsoft (build 3.0.0-25.4.swsoft) allows remote attackers to create and delete arbitrary files as the administrator via a link or IMG tag to (1) create-file and (2) list-control in vz/cp/vzdir/infrman/envs/files/; or modify system configuration via the path parameter to vz/cp/vzdir/infrman/envs/files/index.	2009-03-16	6.8	CVE-2008-6478 XF BID BUGTRAQ SECUNIA OSVDB
parallels -- parallels_virtuozzo	Cross-site request forgery (CSRF) vulnerability in the "change password" feature in the VZPP web interface for Parallels Virtuozzo 25.4.swsoft (build 3.0.0-25.4.swsoft) allows remote attackers to modify the password via a link or IMG tag to vz/cp/pwd.	2009-03-16	6.8	CVE-2008-6479 XF BID BUGTRAQ SECUNIA OSVDB
phpfox -- phpfox	Cross-site request forgery (CSRF) vulnerability in account/settings/account/ in phpFoX 1.6.21 allows remote attackers to change the administrator's email address via the act[update] action.	2009-03-19	6.8	CVE-2009-0969 XF SECUNIA MISC
phpprobid -- php_pro_bid	PHP remote file inclusion vulnerability in includes/class_image.php in PHP Pro Bid 6.05, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the fileExtension parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-19	6.8	CVE-2009-0970 XF BID OSVDB SECUNIA
postgresql -- postgresql	PostgreSQL before 8.3.7, 8.2.13, 8.1.17, 8.0.21, and 7.4.25 allows remote authenticated users to cause a denial of service (stack consumption and crash) by triggering a failure in the conversion of a localized error message to a client-specified encoding, as demonstrated using	2009-03-17	4.0	CVE-2009-0922 CONFIRM MLIST CONFIRM MLIST MLIST

	mismatched encoding conversion requests.			MLIST
prestashop -- prestashop	Multiple cross-site scripting (XSS) vulnerabilities in PrestaShop 1.1.0.3 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to (1) admin/login.php and (2) order.php.	2009-03-20	5.0	CVE-2008-6503 XF BID BUGTRAQ
pro_chat_room -- pro_chat_rooms	Cross-site scripting (XSS) vulnerability in profiles/index.php in Pro Chat Rooms 3.0.2 allows remote attackers to inject arbitrary web script or HTML via the gud parameter.	2009-03-20	5.0	CVE-2008-6501 XF BID MILWORM SECUNIA OSVDB
pro_chat_room -- pro_chat_rooms	Directory traversal vulnerability in Pro Chat Rooms 3.0.2 allows remote authenticated users to select an arbitrary local PHP script as an avatar via a .. (dot dot) in the avatar parameter, and cause other users to execute this script by using sendData.php to send a message to (1) an individual user or (2) a room, leading to cross-site request forgery (CSRF), cross-site scripting (XSS), or other impacts.	2009-03-20	4.0	CVE-2008-6502 XF MILWORM SECUNIA OSVDB
process-one -- ejabberd	Cross-site scripting (XSS) vulnerability in ejabberd before 2.0.4 allows remote attackers to inject arbitrary web script or HTML via unknown vectors related to links and MUC logs.	2009-03-17	4.3	CVE-2009-0934 BID CONFIRM MLIST SECUNIA OSVDB
rhinosoft -- serv-u	The FTP server in Serv-U 7.4.0.1 allows remote authenticated users to cause a denial of service (service hang) via a large number of SMNT commands without an argument.	2009-03-19	4.0	CVE-2009-0967 XF BID MILWORM
robs-projects -- asp_user_engine.net	ASP User Engine.NET stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database via a direct request for users.mdb.	2009-03-19	5.0	CVE-2008-6494 MILWORM
slysoft -- anydvd slysoft -- cloned slysoft -- clonedvd slysoft -- virtualclonedrive	Elaborate Bytes ElbyCDIO.sys 6.0.2.0 and earlier, as distributed in SlySoft AnyDVD before 6.5.2.6, Virtual CloneDrive 5.4.2.3 and earlier, CloneDVD 2.9.2.0 and earlier, and CloneCD 5.3.1.3 and earlier, uses the METHOD_NEITHER communication method for IOCTLs and does not properly validate a buffer associated with the Irp object, which allows local users to cause a denial of service (system crash) via a crafted IOCTL call.	2009-03-14	4.9	CVE-2009-0824 CONFIRM BID BUGTRAQ SECUNIA SECUNIA SECUNIA MISC
	Cross-site request forgery (CSRF) vulnerability in Datalife Engine 6.7 allows			CVE-2008-6480

softnews_media_group -- datalife_engine	remote attackers to perform unauthorized actions as other users via a link or IMG tag to engine/modules/imagepreview.php with a modified image parameter.	2009-03-16	6.8	OSVDB XF BUGTRAQ OSVDB
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the keysock kernel module in Solaris 10 and OpenSolaris builds snv_01 through snv_108 allows local users to cause a denial of service (system panic) via unknown vectors related to PF_KEY socket, probably related to setting socket options.	2009-03-16	4.7	CVE-2009-0913 SECTRACK BID SUNALERT SECUNIA
sun -- opensolaris sun -- solaris	Unspecified vulnerability in Sun OpenSolaris snv_39 through snv_45, when running in 64-bit mode on x86 architectures, allows local users to cause a denial of service (hang of UFS filesystem write) via unknown vectors related to the (1) ufs_getpage and (2) ufs_putapage routines, aka CR 6442712.	2009-03-17	4.7	CVE-2009-0924 VUPEN BID SUNALERT
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the UFS filesystem functionality in Sun OpenSolaris snv_86 through snv_91, when running in 32-bit mode on x86 systems, allows local users to cause a denial of service (panic) via unknown vectors related to the (1) ufs_getpage and (2) ufs_putapage routines, aka CR 6679732.	2009-03-17	4.9	CVE-2009-0926 VUPEN BID SUNALERT
symantec -- pcanywhere	Format string vulnerability in Symantec pcAnywhere before 12.5 SP1 allows local users to read and modify arbitrary memory locations, and cause a denial of service (application crash) or possibly have unspecified other impact, via format string specifiers in the pathname of a remote control file (aka .CHF file).	2009-03-18	4.6	CVE-2009-0538 CONFIRM
tizag -- tizag_countdown_creator	Unrestricted file upload vulnerability in process.php in Tizag Countdown Creator 3 allows remote attackers to execute arbitrary code by uploading a file with an executable extension via index.php, then accessing the uploaded file via a direct request to the file in pics/. NOTE: some of these details are obtained from third party information.	2009-03-19	6.8	CVE-2008-6492 XF BID MILWORM SECUNIA OSVDB
tor -- tor	Unspecified vulnerability in Tor before 0.2.0.34 allows attackers to cause a denial of service (infinite loop) via "corrupt votes."	2009-03-17	5.0	CVE-2009-0936 MLIST
tor -- tor	Unspecified vulnerability in Tor before 0.2.0.34 allows directory mirrors to cause a denial of service via unknown vectors.	2009-03-17	5.0	CVE-2009-0937 MLIST
tor -- tor	Unspecified vulnerability in Tor before 0.2.0.34 allows directory mirrors to cause a denial of service (exit node crash) via	2009-03-17	5.0	CVE-2009-0938 MLIST

	"malformed input."			MILWORM
wordpress -- wordpress_mu	Cross-site scripting (XSS) vulnerability in the choose_primary_blog function in wp-includes/wpmu-functions.php in WordPress MU (WPMU) before 2.7 allows remote attackers to inject arbitrary web script or HTML via the HTTP Host header.	2009-03-19	4.3	CVE-2009-1030 XF SECTRACK BUGTRAQ MILWORM
xlinesoft -- phprunner	UserView_list.php in PHPRunner 4.2, and possibly earlier, stores passwords in cleartext in the database, which allows attackers to gain privileges. NOTE: this can be leveraged with a separate SQL injection vulnerability to obtain passwords remotely without authentication.	2009-03-19	5.0	CVE-2009-0964 XF BUGTRAQ MILWORM MISC
zirkon_box -- yappa-ng	Cross-site scripting (XSS) vulnerability in index.php in Fritz Berger yet another php photo album - next generation (yappa-ng) 2.3.2 allows remote attackers to inject arbitrary web script or HTML via the album parameter.	2009-03-19	4.3	CVE-2008-6495 XF BID SECUNIA MISC
Back to top				

There were no low vulnerabilities recorded this week.